A Domain-Specific Language for Multi-task Systems, applying Discrete Controller Synthesis

Gwenaël Delaval, Éric Rutten

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A Domain-Specific Language for Multi-task Systems, applying Discrete Controller Synthesis

Gwenaël Delaval — Éric Rutten

N° 5690

October 25, 2005

Thème COM

ISSN 0249-6399

A Domain-Specific Language for Multi-task Systems, applying Discrete Controller Synthesis

Gwenaël Delaval*†, Éric Rutten‡

Thème COM — Systèmes communicants
Projets POP ART et DaRT

Rapport de recherche n° 5690 — October 25, 2005 — 44 pages

Abstract: We propose a simple programming language, called Nemo, specific to the domain of multi-task real-time control systems, such as in robotic, automotive or avionics systems. It can be used to specify a set of resources with usage constraints, a set of tasks that consume them according to various modes, and applications sequencing the tasks. We obtain automatically an application-specific task handler that correctly manages the constraints (if there exists one), through a compilation-like process including a phase of discrete controller synthesis. This way, this formal technique contributes to the safety of the designed systems, while being encapsulated in a tool that makes it useable by application experts. Our approach is based on the synchronous modelling techniques, languages and tools.

Key-words: Real-time systems, safe design, domain-specific language, discrete control synthesis, synchronous programming.

* MENRT grant (INPG)
† Gwenael.Delaval@inrialpes.fr, http://www.inrialpes.fr/pop-art/people/delaval
‡ INRIA Futurs/LIFL, Eric.Rutten@inria.fr, http://www.lifl.fr/~rutten

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier (France)
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Un langage spécifique au domaine des systèmes multi-tâches, appliquant la synthèse de contrôleurs discrets

Résumé : Nous proposons un langage de programmation simple, appelé Nemo, spécifique au domaine des systèmes de contrôle-commande temps-réel multi-tâches, tels qu'on les trouve dans les systèmes robotiques, automobiles ou avioniques. Ce langage permet de spécifier un ensemble de ressources avec des contraintes d'utilisation, un ensemble de tâches qui les consomment selon divers modes, et des applications qui séquencent les tâches. Nous obtenons automatiquement un gestionnaire de tâches, spécifique à l'application, qui traite correctement les contraintes (s'il en existe un), au moyen d'un processus de compilation comprenant une phase de synthèse de contrôleurs discrets. De cette façon, cette technique formelle contribue à la sûreté des systèmes ainsi conçus, tout en étant encapsulée dans un outil qui la rend utilisable par les spécialistes des applications. Nous nous plaçons dans le cadre des techniques de modélisation, langages et outils synchrones.

Mots-clés : Systèmes temps-réel, conception sûre, langage spécifique au domaine, synthèse de contrôleurs discrets, programmation synchrone.

1 Context and motivation

1.1 Embedded control systems and tasks

Embedded control systems are implementing automatic control laws or signal processing, such as in robotic, automotive or avionics systems, or even more widely available portable devices processing voice and image signal. These systems are reactive, working in close interaction with their environment, including the controlled process, which has its own dynamics (typically, following the laws of physics), imposing real-time management. The global behavior of such control systems results from this very interaction.

They are typically designed in terms of continuous models, and then implemented in a dicretized form, as a *cyclic* computation upon sensor input data, producing extracted information, or control values towards actuators. This combination of computations and resource usage (sensors, processors, memory, power, actuators) defines a level of abstraction which we call a *task*.

For a complex system, with a number of different resources and meant to fulfill a variety of functionalities, several control *modes* or *phases* can be designed, and the switching between them has to be handled and controlled properly [12]. This can be intricate and the risk of errors is important, because of the complexity of systems and of requirements, particularly with respect to constraints on resource usage and interaction with the environment. Task handlers can be seen as property-enforcing layers [1]. Instances of systems structured this way can be found in robotics e.g., in robot programming environments like Orccad [4]. Programming languages for such purposes typically combine data-flow and sequencing [23, 18, 17]. The same kind of abstraction level, considering the control of tasks independently of the encapsulated computation, is considered in the reactive language Electre [5].

We address the difficulty of designing safely such complex controllers by proposing a method applying safe design techniques to the domain of embedded control systems.

1.2 Safety-critical systems

The systems to be controlled are in interaction with their environment, in such a way that malfunction can lead to disastrous consequences, be it material, financial or human. Hence, their design has to be safe, so that they are correctly constructed and fully validated before being put into operation.

Formal methods and verification are a way to design safety-critical systems with an explicit care for their validation. The design is based on models of requirements, architectures, properties to be satisfied. A common practice consists of building up a specification, and then using *formal verification* techniques (e.g., model checking of temporal logic properties on a transition system-based abstraction of the system) to assess wether given properties are satisfied or not. In the latter case, when a bug is detected, the verification technique can give indications or a diagnosis on its origin, and the designer has to go back to the design and modify it, before performing the verification again.

Such techniques are considered difficult to use, amongst other things because of the competence required in formal techniques. Much effort is devoted to *make them more user-friendly*, because they are to be applied by engineers specialists of the systems under design. A general notion of *hidden formal methods* advocates for fully automated techniques, integrated into a design process and tools. Approaches exist in methods providing with correctness by construction [2], where safe components can be assembled by operations preserving some essential properties like deadlock freedom.

Some *programming languages* have compilers integrating verification e.g., the synchronous languages for reactive systems [9, 10, 3] check for each program whether static properties are satisfied, regarding the coherence of event synchronizations. Explorations of dynamical behaviors in the reachable state space, integrated in the compilation [16, 11] is applied less currently, e.g., for optimisation purposes w.r.t. dead code [21] , or interface computations [6].

For the control systems that we consider, what has to be verified is the correctness of the controller handling switchings between tasks and resources. We propose to use a formal technique, targeted at the level of these controllers, integrated in a user-friendly design framework.

1.3 Synthesis of task handlers

Verification is autopsy. [7]

One formal technique is *discrete controller synthesis* [22]. It can be defined in the framework of formal languages, or finite state automata or transition systems, and it consists of, given a property given as objective, computing the constraint (i.e., the controller) on transitions, if there exists one, such that the resulting constrained (i.e., controlled) behavior satisfies the property. It can be defined on algorithmic bases similar to those for model checking. It differs from verification in that it is

more constructive, and proposes a solution. The technique has been studied and implemented in the synchronous framework [19].

It has been applied to the *modelling and control of multi-task systems* [2, 20, 14, 24], where the set of tasks is modelled as a transition system, and a controller has to be found that handles the preservation of constraints regarding the resources and sequencing. It can then be seen as the automatic generation of a *property-enforcing layer* [1] for a given system, or of an *application-specific scheduler* [15].

Our aim is to adapt these models and applications of discrete controller synthesis to multi-task control systems, in a way such that it is encapsulated into a simple domain-specific language, and an automatic generation framework.

1.4 Our approach

We propose a *domain-specific language*, called NEMO, encapsulating controller synthesis for multi-task systems. Its constructs describe domain-specific notions of resources and their constraints, tasks and their control, particular ordering constraints to be enforced, and applications built upon them. It is defined in terms of transition systems, temporal properties, and synthesis objectives. We produce, through a compilation-like process including a phase of discrete controller synthesis, i.e., *automatically*, a *correct application-specific task handler* that satisfies the constraints (if there exists one). This way, this formal technique contributes to the safety of the designed systems, while being encapsulated in a tool that makes it useable by programmers. We use synchronous languages, modelling techniques and tools, particularly we use the Mode Automata language [17] and the Sigali synthesis tool [19].

Our contribution is in the proposal of this language, and the "hidden" use of discrete controller synthesis, which we apply as such, in a fairly basic way.

In the remainder of this paper, section 2 exposes motivations for the language's constructs. Section 3 gives an informal overview of this language. Section 4 gives a detailed description of all the language constructs, with associated transitions systems and synthesis objectives: preliminary definitions are given in Section 4.1. Section 4.2 describes how tasks are modelled, followed by resources in section 4.3. Section 4.4 describes temporal properties, section 4.5 describes how applications are assembled from the preceding ingredients. In section 5, the implementation using synchronous tools is presented. Section 6 illustrates the approach with an example. Performance aspects are discussed in section 5.2. Section 7 concludes.

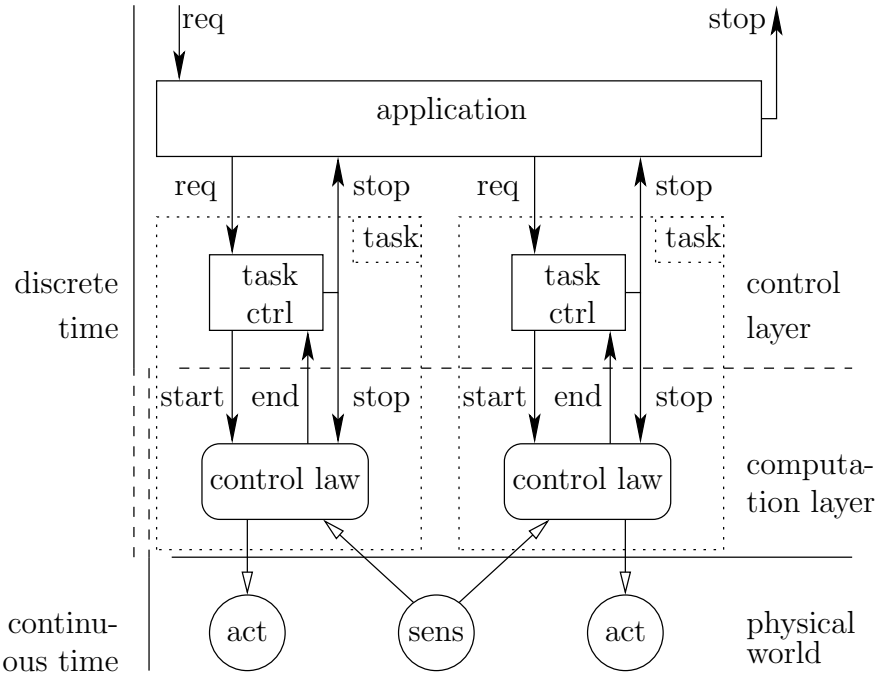


Figure 1: Control system composed of computations encapsulated into tasks, topped with an application

2 Analysis of the domain specificities

This section gives motivations for the further language's constructs in terms of the targeted class of systems.

2.1 Computations, tasks, applications

We consider control systems composed of two layers.

- The *computation layer* performs data transformation algorithms, e.g. numerical computations, in an infinite loop. These computations can be implemented as C code, and, as shown in the lower part of figure 1, have basic control points:
  - they can be *started*, which can involve initializations;
  - they can *signal that they have reached their end*: i.e., they are ready to stop: e.g., a control law has reached its objective within a given precision

range (it may yet not stop but continue controlling the actuator around the objective);
  - they can be *stopped*: e.g., interrupted;
  - they can be *suspended* i.e., they cease computation and interaction, until they are resumed.

- The *control layer* manages these computations' starts and stops, by encapsulating them into *tasks*, each provided with a local controller. As shown in the middle part of figure 1, this controller makes the relation between requests and starts, and between ends and stops: as will be discussed below, several variants may make sense. A task can also involve several *modes of activity*, where the computation is different, as well as the resources engaged.

  These tasks can then be composed into *applications*, using structures such as loops, sequences, or parallel statements. As shown in the upper part of figure 1, it can be requested, and send in turn, according to its control structure, requests to underlying tasks, and can eventually stop.

  This whole *control* layer is a discrete event system, we see it as a synchronous reactive system [3].

2.2 Resources

Such computations are related to *resources*,

- for their computation: typically processors, memories, communication links;
- and in the embedded system: typically sensors, actuactors.

These resources involve *constraints* which are implicit properties such as:

- exclusivity,
- bounds on the number of users,
- bounds on the available capacity,
- the need to be always under control.

Within a task, modes can correspond to several different configurations w.r.t. resource consumption, e.g., with choices between time and memory consumption, degraded modes with lower quality level but also lower consumption.

The application defines a sequencing of tasks by constructing a controller that interacts with the tasks local controllers, and the global controller hence constructed has to *preserve* the properties of the resources.

2.3 The points to be controlled

We will here describe different possible articulations between ends, stops, requests and starts, which will motivate the constructs of the Nemo language presented further. They correspond to different kinds of computations that can be seen in applications.

2.3.1 Controlling the termination of a computation

As we said, the end reports the reaching of some termination condition, the stop is the actual termination of the computation. Controlling the termination of a computation involves relating *stops* and *ends*.

Stop coming before end Some computations may be stopped without having yet reached their complete termination: e.g., anytime algorithms, characterized by an incremental construction where each intermediary result can be delivered as a result, be it of intermediary quality. Such tasks can hence be interrupted before having reached an end: their *stop can be triggered*.

Stop coming after end Some computations reach their objective, and they can continue cyclically in order to maintain it: an example is a control law, always giving the correction to be applied by actuators in order to near the objective. When the latter is reached, continuing will just maintain the situation. This can be useful and even necessary: for example, in Orccad[4], the Robot-Tasks encapsulating a control law have a "transition phase" when the task is finished, but the next task isn't yet started: the task executes a "degraded mode" until the start of the next task, thus allowing the operation of actuators that have to be always under control. Such tasks can hence be sustained beyond their end: their *end can be rejected*: the stop will occur at a later occurrence of the end, or *delayed*: the stop occurs at a later point, even without re-occurrence of the end.

2.3.2 Controlling the beginning of a computation

As for the termination, controlling the beginning of a computation involves relating *requests* and *starts*.

Start coming after request When a request is made for a task, it might not be started, typically because of a resource not being available yet. Then, the request may be memorized for later treatment, or not. The *request* can be *rejected*: the start will occur at a later occurrence of the request, or *delayed*: the start occurs at a later point, even without occurrence of the request.

Start coming before request Some computations may be called without an explicit request being made, for example default control tasks for an actuator that must always be under control: their *start* can be *triggered*.

2.3.3 Controlling the modes during a computation

involves switching between them. Modes are different ways to achieve the functionality of a task, which vary in the resources they consume, the time they take, the quality of service they achieve. For example, on an architecture composed of two processors P_1 and P_2, some tasks can be executed on either P_1 or P_2. So, we can say that this task is composed of two modes, each of them corresponding to the execution of the task on a given processor. Another example is a computation that can be performed by several algorithms, each of them using different amount of the available resources.

Switching modes can have the effect of e.g., making space in a bounded resource for other tasks to be able to begin, or to switch to a better quality and more costly mode, or unlocking a task waiting upon an exclusive resource.

The mode switches are part of the control points available to the controller to be synthesized.

3 Overview of the language

This section gives an informal overview of the Nemo language, taking into account the analysis performed in section 2.

3.1 Programming multi-tasks systems with Nemo

The Nemo language is devoted to build control layers. It allows for describing an abstraction of the computation layer, i.e. the *resources* used, the ways computations can be controlled i.e., *tasks*, some *explicit temporal properties* between *tasks*. These declarations are used to specify an *application*, in terms of an imperative sequencing of tasks.

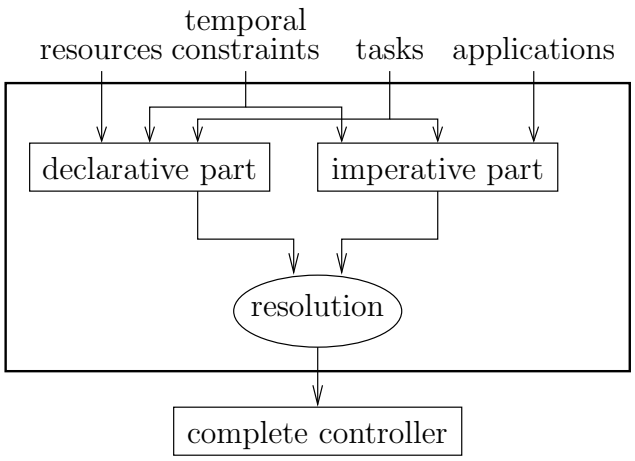


Figure 2: Compilation of Nemo.

From these elements, two basic elements are to be derived, as shown in figure 2:

- a *declarative part*, grouping
  - the constraints corresponding to resources,
  - the explicit properties to be enforced,
  - the declared consumptions of tasks.
- an *imperative part*, grouping
  - the observers for the explicit properties,
  - the behaviors of the tasks,
  - the behaviors of the applications.

These two parts constitute a partial specification. The imperative part features behaviors not satisfying a priori the constraints in the declarative part, with some

points to be controlled. Therefore, obtaining the complete controller, satisfying these properties, involves applying some *resolution*.

This requires the use of formal models and algorithms, in order for the process to be automated, and encapsulated into a compiler-like tool. In our approach, the models will be autoamata, and the resolution will take the form of discrete controller synthesis.

In the following, we will introduce the programming constructs of the language in an informal way, from a user's view. Further sections will give the definitions in terms of transition systems, and properties and synthesis objectives.

3.2 Resources: implicit properties

A resource is declared using the keywords `resource` and `end resource`, with properties as follows. These properties are all optional, and can be specified in any order.

Bounded number of users This maximum number of tasks which can use the resource at the same time is stated by `usable by` n `tasks`, where n is a natural integer. For example, a resource declared as :

```
resource actuator:
    usable by 2 tasks;
end resource;
```

can be used by no more than 2 tasks.

Exclusivity is the particular case where $n = 1$.

Bounded capacity A "decomposable" resource, composed of elements which can be distributed among the tasks using it (e.g. a memory), is declared by mean of the construct `composed of` n `elements`. Uses of such a resource will be quantified, and bounded by n.

Steady control Some resources have to be controlled by *at least one task*, e.g. actuators in a robotic system. This is stated by `steady control`.

Example. The following example shows the definition of a resource usable by at least one task, at most 3 tasks, and decomposable in 42 elements.

```
resource r:
    usable by 3 tasks;
    composed of 42 elements;
    steady control;
end resource;
```

3.3 Tasks

A task is declared by `task`, followed by the task name and a colon, and `end task`. This construct encloses a list of task properties, separated by semi-colons, as follows.

3.3.1 Activity

A task's *activity* of a task involves three notions.

Properties of the beginning of the task As exposed in 2.3.2, a task can be stated as *beginning-triggerable*, *beginning-delayable* and *beginning-rejectable*. They are specified by the keyword `start`, followed by one or more of `triggerable`, `delayable` and `rejectable`. Due to their incompatible meanings, the two options `delayable` and `rejectable` are exclusive.

A *beginning-triggerable* and *beginning-delayable* task `go` will then be specified as:

```
task go:
    start triggerable, delayable;
    ...
end task;
```

Properties of the end of the task are specified by the use of the keyword `stop`, followed by the same keywords as for beginning properties.

Suspensibility means that computation can be suspended at any instant by the task controller. Thus, resources used can be declared as used only when the computation is actually running, or always used (i.e., kept reserved and busy during the suspension). A suspensible task is specified by `suspensible`.

```
task think:
    suspensible;
end task;
```

3.3.2 Resources used by a task

Usage of resources is specified by `uses`, followed by the names of the resources used. If the resource is used even when the task is suspended, it is specified by the keyword `always`. The use of a decomposable resource is specified by n `of`, followed by the name of the resource.

The following example shows how a task using three resources can be declared. This task, named `go_forward`, uses a resource named `wheels`, 50 elements of a resource named `cpu`, and always 20 elements of the resource `memory`. This example also illustrate the possible meaning of decomposability of a resource.

```
task go_forward:
    uses wheels;
    uses always 20 of memory;
    uses 50 of cpu;
end task;
```

3.3.3 Modes composing a task

A definition of a set of modes is surrounded by the keywords `modes` and `end modes`. Thus, orthogonal aspects of a tasks can be specified by means of different sets of modes, with several such constructs.

The definition of each mode is composed of its name, and what resources it uses (specified by `uses` as shown above).

Transitions between modes are not necessarily all possible. For example, in the case of three modes for high, medium and low values of some characteristics, one can go from high to low only through medium. So each transition has to be specified explicitely. Also, we make the choice that transitions are all bi-directional, and unconditioned (i.e., controlled entirely by the controller to be synthesized). A transition between the two modes A and B is specified as `trans A <-> B;`.

Example. The following example is the specification of a task encapsulating a computation which can be performed by three different algorithm versions, here named `high`, `medium` and `low`. It shows also how to deal with compromises such as CPU vs memory use, by having the synthesized controller decide when to use what algorithm version, i.e., in this example, to switch between the `high` and `medium` algorithms, and between the `medium` and `low` ones.

```
task calc1 :
  start rejectable;
  modes
    high : uses 100 of CPU, always 50 of Memory;
    medium : uses 80 of CPU, always 70 of Memory;
    low : uses 50 of CPU, always 80 of Memory;
    trans high <-> medium;
    trans medium <-> low;
  end modes;
end task;
```

In that specific case, expected behavior of the synthesized controller is that, if another task is undelayable and requires 50% of CPU, then it will ensure that the system will never get in the `high` mode of the `calc1` task. Indeed, in this mode, the system couldn't go back directly to the `low` mode in case of the request of the other task.

3.4 Temporal constraints: explicit properties

Until now, the properties considered were all seen through the use constraints declared with the resources. Some other constraints could be required, for reasons not directly related to any declared resource, but having to do with some knowledge about the environment, e.g. the possible incompatibility between some activities for reasons not modelled here (waiting for a temperature to cool down, rinsing brushes between painting in two different colours,...). Therefore, we introduce a few constructs enabling the specification of explicit temporal constraints. Properties expressible in Nemo will be safety temporal properties.

The basic events of those properties are tasks executions: a "task execution" runs from the emission of its "start" signal to the emission of its "stop" signal. The temporal properties will then be expressed in term of observers [11] on these events. Nemo provides five elementary properties patterns, and two logical operators to compose properties.

Always between : Between the executions of the two specified tasks `t1` and `t2`, a third specified task `t3` must always be executed. This is expressed as:

```
property
    always t3 between (t1,t2)
end property;
```

Always before : The execution of a specified task must always be preceded by the execution of another specified task. We can imagine, as example, a physical resource `r` which have to be initialized by executing a task named `init` before any use of `r`. Then, if a task `t` is declared as using `r`, we have to explicitly declare that `init` must be executed before `t`. This is expressed as `always init before t`.

```
property
    always init before t
end property;
```

Always during : During any execution of a task `t1`, the task `t2` must be executed: `always t2 during t1`.

```
property
    always t2 during t1
end property;
```

Always while : The execution of `t1` must always take place while `t2` is in execution: `always t1 while t2`.

```
property
    always t1 while t2
end property;
```

Never while : Execution of two specified tasks `t1` and `t2` are mutually exclusive: `never t1 while t2`.

```
property
    never t1 while t2
end property;
```

Or, and : They are the classical ones. The "not" operator cannot be allowed, so as to stay within safety properties.

3.5 Applications

Applications are the imperative part of NEMO. Their purpose is the expression of an order of execution of the tasks, for a functionality to be produced.

Once we have defined, through the declarative part of the language, a set of resources, tasks, and properties, the interface provided by the system obtained to its environment (i.e. its set of uncontrollable inputs) is, for each task, two requests

signals, respectively requesting the start and the end of the task. These signals can then be received from the environment to the system at any time and in any order.

Applications define an intermediate layer emitting starting requests to task controllers, and waiting for ends of tasks, as shown in figure 1. Compared to the usual intuition in imperative languages, sending a request does not mean activation of the task: the sequencing is to be interpreted as being soft.

The definition of an application is surrounded by the keywords `application`, followed by the application name and a colon, and `end application`. It encloses the application statement, written using the following constructs.

Task or application request will simply be noted by its name (this simple application will just emit the signal `req`, and terminate when it will receive the signal `stop`).

Sequence of two applications app_1 and app_2 is noted :

$$app_1 \texttt{ ; } app_2$$

It requests app_1, then upon termination app_2.

Parallel composition of two applications app_1 and app_2 is noted

$$app_1 \texttt{ || } app_2$$

This requests app_1 and app_2 simultaneously: they can then be executed in any order or at the same time. It terminates when both are terminated.

Alternative between two applications app_1 and app_2 is noted

$$app_1 \texttt{ | } app_2$$

This executes either app_1, or app_2, and terminates whith the chosen application. The choice is left free, for the controller to decide, either at run-time, if both are potentially possible, or off-line, if the preservation of properties excludes one of them.

Trigger of an application *app* by a signal s awaits the occurence of s, then requests *app*. It is noted

$$s \texttt{ triggers } app$$

Loop of an application *app*, executed repeatedly until the occurence of a signal *s*, reads:

`loop` *app* `until` *s*

This requests *app*; once *app* terminates, if *s* is absent, it requests *app* again, and so on. The condition required to get out of a loop may appear rather restrictive, but one can see that they could be emitted from observers [11, 13] in a general way.

Here is a small example of use of this application language: the application `A2` is a loop, which executes repeatedly the task `T3`, then the tasks `T4` and `T5` in any order, and then the application `A1` which executes either `T1` or `T2`.

```
application A1 :
    T1 | T2
end application;

application A2 :
    loop
        T3 ; (T4 || T5) ; A1
    until kill_A2
end application;
```

3.6 Compiling a Nemo program

Now that the Nemo language is defined, its compilation towards a complete controller will have to start from a set of resources, temporal constraints, tasks, and applications, as shown in figure 3, which can be seen as a refinement of figure 2.

Based on such a program, a compilation-like process constructs an *automaton*-based model of behaviors to be controlled, featuring *free variables* for the points to be controlled, and a set of properties derived from the declared constraints are giving *objectives* for the synthesis. *Discrete controller synthesis* is applied on them. It computes the *controller* i.e., the constraints on the control points of the tasks which are necessary for the properties or objectives to be fulfilled. This way, the *controlled automaton*, such that the properies are satisfied, can be used through the *co-execution* or co-simulation engine.

This way, we achieve a form of *hidden formal method*, not of course out of shame, but as a relief for users from heavy prerequisites in difficult technicalities of the formal method applied.

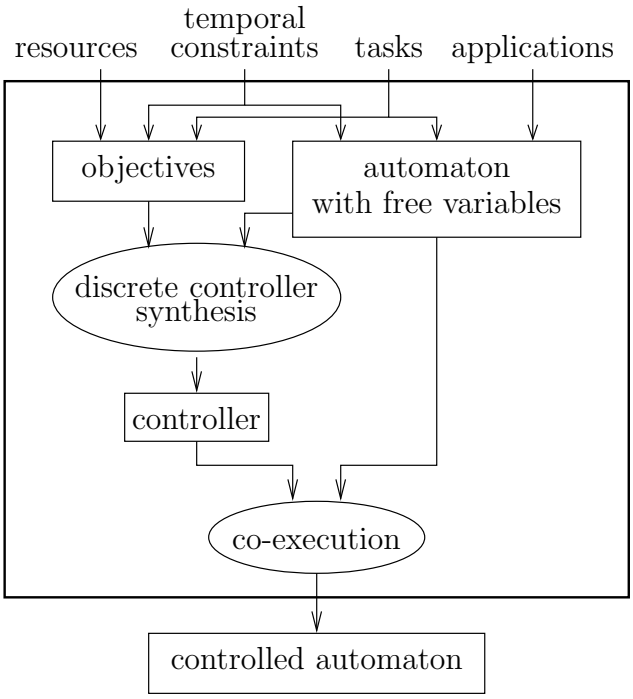


Figure 3: Compilation of NEMO: models and algorithms.

4 Modelling behaviors and properties

This section presents the formal modelling of NEMO. The behavioral aspects will be defined in terms of labeled transition systems, with a synchronous composition operator as in synchronous languages [3, 9, 10]. Properties on states and trajectories will be used to give objectives to the controller synthesis; when concerning sequences of transitions or states, these are defined in terms of observers , themselves introducing transition systems composed with the previous ones [1].

4.1 Preliminary definitions

We give just a very brief recall of notions used here, in a classical way, and which are further detailed elsewhere [1].

4.1.1 Transition systems

The labelled transition systems we use in this paper are Mealy automata. An automaton $\mathcal{A}$ is a tuple $\mathcal{A} = \langle \mathcal{Q}, s_{init}, \mathcal{I}, \mathcal{O}, \mathcal{T} \rangle$ where $\mathcal{Q}$ is the states set, $s_{init} \in \mathcal{Q}$ the initial state, $\mathcal{I}$ and $\mathcal{O}$ the input and output variables sets, and $\mathcal{T} \subseteq \mathcal{Q} \times \mathcal{B}ool(\mathcal{I}) \times 2^{\mathcal{O}} \times \mathcal{Q}$ the transitions set. $\mathcal{B}ool(\mathcal{I})$ is the set of boolean expression with variables in $\mathcal{I}$. We note $\mathcal{A}_1 \| \mathcal{A}_2$ the synchronous composition [3, 9, 10, 1] of the two transition systems $\mathcal{A}_1$ and $\mathcal{A}_2$. If $\mathcal{A} = \mathcal{A}_1 \| \ldots \| \mathcal{A}_n$ and $s_i \in \mathcal{Q}_i$, we note $\underline{s_i}$ the subset of $\mathcal{Q}$ whose projection in $\mathcal{Q}_i$ is equal to s_i. $\overline{s_i}$ denotes the complementary of $\underline{s_i}$ in $\mathcal{Q}$. A states set $\mathcal{Q}' \subset \mathcal{Q}$ is an *invariant set for* $\mathcal{A}$ iff every eligible transition outgoing from states of $\mathcal{Q}'$ lead to a state of $\mathcal{Q}'$.

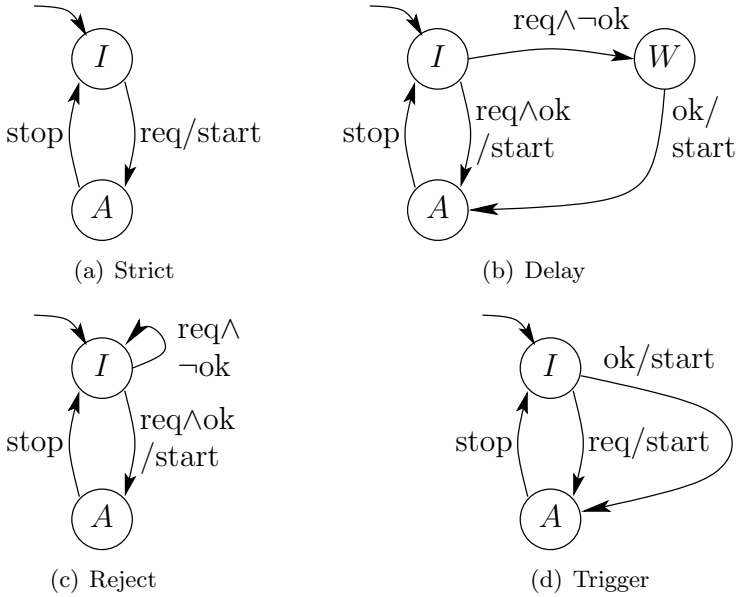
4.1.2 Weight functions

We are going to describe properties of states by mean of *weight functions*. A weight function on a states set $\mathcal{Q}$ is a function $f : \mathcal{Q} \to \mathbb{N}$ assigning a value to each state of the transition system. We will manipulate such functions using addition and multiplication of two functions, and product of a function by a scalar λ, whith the usual meaning: $(\lambda.f)(q) = \lambda.f(q)$, $(f+g)(q) = f(q)+g(q)$ and $(f.g)(q) = f(q).g(q)$. Furthermore, all the weight functions considered below take their image on the states set resulting of the general composition of all the automata.

4.1.3 Discrete controller synthesis

We simply use the classical notion, without modifying it in this work [22, 1]. The aim of the discrete controller synthesis is, from an automaton $\mathcal{A}$, to compute a controller $\mathcal{C}$ such that $\mathcal{A} \| \mathcal{C}$ satisfies a property P, called *synthesis objective*, not satisfied *a priori* by $\mathcal{A}$. For $\mathcal{A} = \langle \mathcal{Q}, s_{init}, \mathcal{I}, \mathcal{O}, \mathcal{T} \rangle$, and a partition of its inputs variables into two subsets $\mathcal{I}^c$ (the *controllable* inputs) and $\mathcal{I}^u$ (the *uncontrollable* ones), a *controller* of $\mathcal{A}$ is an automaton $\mathcal{C} = \langle \mathcal{Q}, s_{init}, \mathcal{I}^u, \mathcal{O} \cup \mathcal{I}^c, \mathcal{T}' \rangle$ such that $\exists (s, \ell_u \wedge \ell_c, O, s') \in \mathcal{T} \iff \exists \gamma \subseteq \mathcal{I}^c \wedge \exists (s, \ell_u, O \cup \gamma, s') \in \mathcal{T}'$, where ℓ_u (respectively ℓ_c) holds only variables of $\mathcal{I}^u$ (resp. $\mathcal{I}^c$) and γ holds at most the controllable inputs of ℓ_c.

Tools and algorithms exist, e.g., in the synchronous approach [19], which we use as they are. A detailed discussion of their principles is out the scope of this paper. We use only the *invariance* objective, i.e., the properties to be satisfied are all invariance properties: for an automaton $\mathcal{A}$, we note $Inv(S)$ the controller $\mathcal{C}$ such that S is invariant for $\mathcal{A} \| \mathcal{C}$.



(a) Strict (b) Delay

(c) Reject (d) Trigger

Figure 4: Models of tasks beginnings

4.2 Tasks: behaviours

We are going to show how to build, from the properties of a task t, an automaton $\mathcal{A}^t$ modelling the behavior of t.

4.2.1 Beginning of the task

It is related to a request, coming from, e.g., the application automaton, as will be defined further, and being an uncontrollable signal `req`. The task controller will emit a `start` signal to actually launch the computation encapsulated in the task. In order to express the controllability on the beginning of the task, we introduce a controllable signal named `ok`, which will control the emission of `start` of tasks with a non-strict beginning (i.e., delayable or rejectable).

The behavior of a task with a *strict* beginning is defined by the automaton on the figure 4(a). The "start" signal is emitted when "req" occurs; there is no means to inhibit it.

A "non-strict" beginning means that the request can be:

- *delayable*: the task controller will memorize it, as in figure 4(b);

- *rejectable*: the task can only begin in the presence of a request, and and will wait for the next occurrence, as in figure 4(c).

A "*triggerable*" beginning means that the computation can be launched by the task controller without request from the environment, as in figure 4(d). This property is very useful to define default task controlling resources which have to be continuously controlled.

To this automaton $\mathcal{A}^t_{beg}$, we associate a weight function

$$\mathcal{W}^t_{beg}(q) = \begin{cases} 1 & \textit{if } q \in \underline{A}, \\ 0 & \textit{otherwise.} \end{cases}$$

4.2.2 End of the task

It involves a similar modelling: a signal called `end` is received (e.g., from the computation itself). The task controller will emit a `stop` signal to actually stop the computation, and report the actual end of the task to the environment. We use the same controllable input `ok` to control the emission of `stop` with respect to occurrences of `end` and properties of the task. This automaton is $\mathcal{A}^t_{end}$.

Figures 5(a) to 5(d) show the models of ends of tasks.

4.2.3 Suspensibility of the task

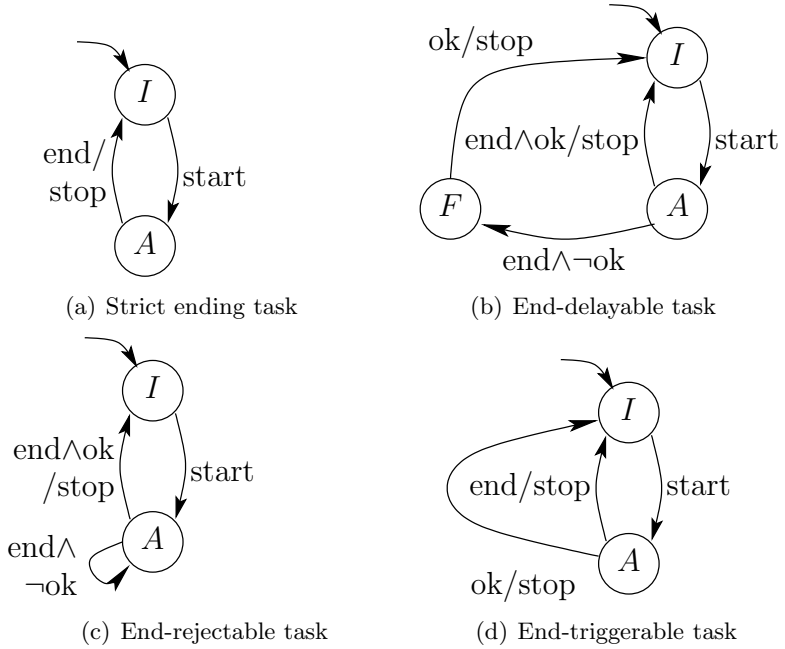
It is modeled by the automaton $\mathcal{A}^t_{susp}$ of figure 6, to be composed with the previous ones. A new controllable input `susp` allows for switching between the "active" and the "suspended" state. We associate to it a weight function $\mathcal{W}^t_{susp}$ defined as:

$$\mathcal{W}^t_{susp}(q) = \begin{cases} 1 & \textit{if } q \in \underline{A}, \\ 0 & \textit{otherwise} \end{cases}$$

4.2.4 Modes

They will be modelled as a new automaton, in parallel with the previous ones. It comprises an "idle" state, one state s_m for each mode m, and controllable transitions between the modes reachable from each other.

Figure 7 shows the automaton representing the set of modes as defined in the example of section 3.3.3: l, m and h are controllable inputs which allow the task controller to control the mode in which the task is executed. We use here one input per mode for the sake of readability, but for determinism we actually assign to each mode m an expression ℓ_m, such that $\forall(m_1 \neq m_2)\ \neg(\ell_{m_1} \wedge \ell_{m_2})$.



(a) Strict ending task (b) End-delayable task

(c) End-rejectable task (d) End-triggerable task

Figure 5: Models of tasks ends

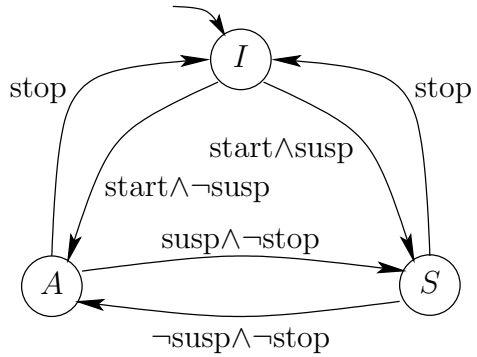


Figure 6: Model of the suspension of a task

For each mode m, we note t_m the task concerning m, with and we associate to m a weight function $\mathcal{W}_m$ defined as (s_m stands for the state representing the mode

in the automaton modelling the set of modes which contains m):

$$\mathcal{W}_m(q) = \begin{cases} 1 & \textit{if } q \in \underline{s_m}, \\ 0 & \textit{otherwise}; \end{cases}$$

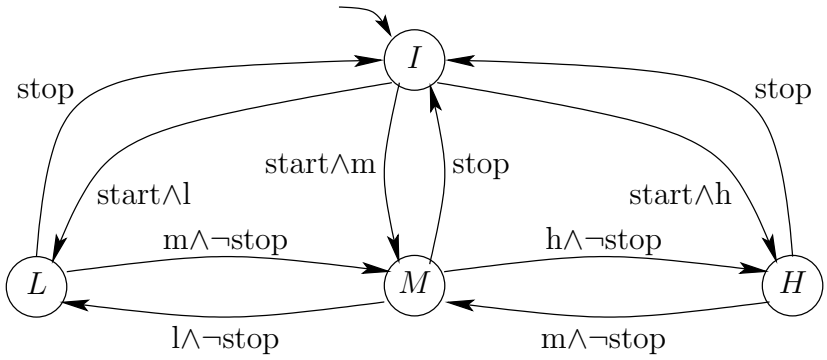


Figure 7: Model of three modes of a task

4.2.5 Global behavior of the task

The definition of the automaton $\mathcal{A}^t$, modelling the global behavior t is then deduced from above is:

$$\mathcal{A}^t = \mathcal{A}^t_{beg} \| \mathcal{A}^t_{end} \| \mathcal{A}^t_{susp} \| \mathcal{A}^t_{M_1} \| \dots \| \mathcal{A}^t_{M_n}$$

where the $\mathcal{A}^t_{M_i}$ are the modelling each modes set M_i of the task t. This automaton is also given in figure 8

4.3 Resources: implicit properties and synthesis objectives

Now that the behavior of tasks are specified in term of transition systems, we are going to show what implicit properties can be deduced from the resources and tasks properties, and are translated in terms of synthesis objectives.

4.3.1 Notations

We will consider that $\mathcal{T}$ and $\mathcal{R}$ are respectively the sets of the tasks and resources composing the system. For $r \in \mathcal{R}$, $\mathcal{T}^r$ is the set of tasks which use r, partitioned in two subsets $\mathcal{T}^r_{alw}$ and $\mathcal{T}^r_{act}$ the sets of tasks using r, respectively, *always* (specified

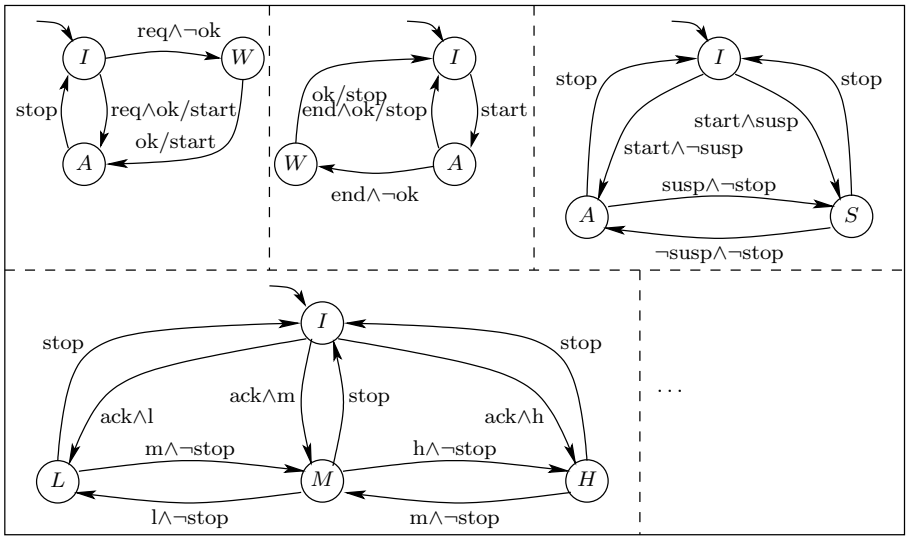


Figure 8: Complete model of a task

by `always` with `suspensible`), and *only when active*. In the same way, we note $\mathcal{M}$ the set of all modes, $\mathcal{M}^r$ the set of modes using r partitioned as well in two subsets $\mathcal{M}^r_{alw}$ and $\mathcal{M}^r_{act}$.

For all decomposable resources r, we define the functions $ET^r : \mathcal{T}^r \to \mathbb{N}$ and $EM^r : \mathcal{M}^r \to \mathbb{N}$ where $ET^r(t)$ (resp. $EM^r(m)$) is the number of elements of r used by the task t (resp. in the mode m).

We also define the two functions:

- $\mathcal{N} : \mathcal{R} \to \mathbb{N}$ where for $r \in \mathcal{R}$, $\mathcal{N}(r)$ is the maximum number of tasks which can use r at the same time;
- $\mathcal{E} : \mathcal{R} \to \mathbb{N}$ where for $r \in \mathcal{R}$, $\mathcal{E}(r)$ is the number of elements composing r.

4.3.2 Synthesis objectives

Bounded number of resource users is handled by a function $\mathcal{U}^r : \mathcal{Q} \to \mathbb{N}$, associating a weight $\mathcal{U}^r(q)$ on each state q of the global system, representing the number of tasks using r in the state q. $\mathcal{U}^r$ can easily be computed by means of the functions introduced above:

$$\mathcal{U}^r = \sum_{t \in \mathcal{T}^r_{alw}} \mathcal{W}^t_{beg} + \sum_{t \in \mathcal{T}^r_{act}} \mathcal{W}^t_{susp} + \sum_{m \in \mathcal{M}^r_{alw}} \mathcal{W}_m + \sum_{m \in \mathcal{M}^r_{act}} \mathcal{W}_m . \mathcal{W}^{t_m}_{susp}$$

Then, to preserve the implicit property that the resource r will not be used by more tasks than it can hold, the computed controller must ensure that the system will stay within the set of states q such that $\mathcal{U}^r(q) \leq \mathcal{N}(r)$.

So, the synthesis objective to compute so as to ensure the property of bounded number of users of r is:

$$Inv(\{q \in \mathcal{Q} | \mathcal{U}^r(q) \leq \mathcal{N}(r)\})$$

Exclusiveness is just the special case where $\mathcal{N}(r) = 1$.

Distinguishing this case is worthwhile, as the synthesis objective can be expressed only in terms of states exclusiveness, into boolean formulas, computable much more efficiently.

Continuous control for r corresponds to the objective

$$Inv(\{q \in \mathcal{Q} | \mathcal{U}^r(q) \geq 1\})$$

There again, it can be formulated in a boolean formula.

Decomposable resources r are handled with a function $\mathcal{C}^r : \mathcal{Q} \to \mathbb{N}$, where $\mathcal{C}^r(q)$ giving the total amount of elements of r consumed by the tasks using r in the state q:

$$\begin{aligned} \mathcal{C}^r = & \sum_{t \in \mathcal{T}^r_{alw}} \mathcal{ET}^r(t).\mathcal{W}^t_{beg} + \sum_{t \in \mathcal{T}^r_{act}} \mathcal{ET}^r(t).\mathcal{W}^t_{susp} \\ + & \sum_{m \in \mathcal{M}^r_{alw}} \mathcal{EM}^r(m).\mathcal{W}_m + \sum_{m \in \mathcal{M}^r_{act}} \mathcal{EM}^r(m).\mathcal{W}_m.\mathcal{W}^{t_m}_{susp} \end{aligned}$$

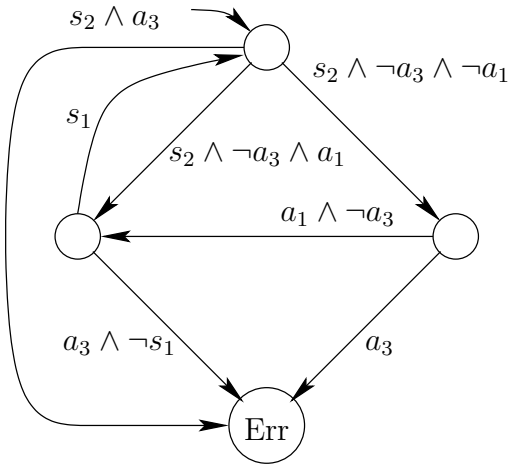
Then, the controller is

$$Inv(\{q \in \mathcal{Q} | \mathcal{C}^r(q) \leq \mathcal{E}(r)\})$$

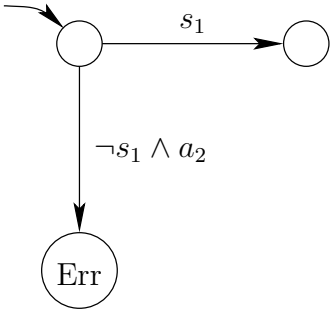
4.4 Temporal constraints: explicit properties

Observers and objectives. They are translated into observer autmata, describing sequences leading to an "error" state Err where they are violated. The synthesis objective is the invariance of the state set deprived of this "error" state: $Inv(\overline{Err})$

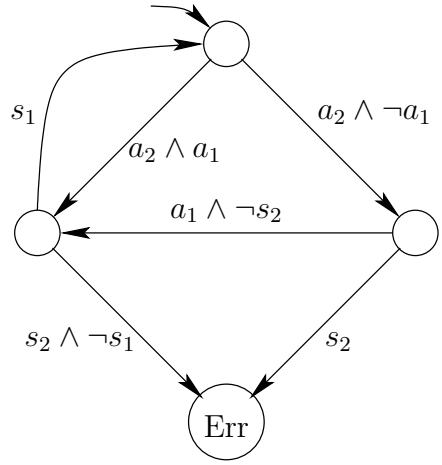
The observers are placed in parallel with the automata managing the tasks. They will take as inputs the "start" (a_i) and "stop" (s_i) signals of the tasks they observe.



(a) `always t1 between (t2,t3)`



(b) `always t1 before t2`



(c) `always t1 during t2`

Figure 9: Observers for the temporal constraints

"Always between" observer. Figure 9(a) depicts the observer for the property:

```
always t1 between (t2,t3)
```

The state "Err" is reached when a_3 occurs after s_2, unless a_1 then s_1 are emitted in between.

"Always before" observer. The figure 9(b) depicts the observer for the property

```
always t1 before t2
```

The "Err" state of this observer is unreachable once `t1` has been executed.

"Always during" observer. The figure 9(c) depicts the observer for the property

```
always t1 during t2
```

This observer is very similar, and can easily be compared with the observer of the "between property" (figure 9(a)). The differences are due to taking into consideration that a task lasts at least one instant.

"Always while" property. This property doesn't need adding an observer. Actually, the property "t_1 is executed always while t_2 is executed" is strictly equivalent to "the model automaton of t_1 is in an execution state $\Longrightarrow$ the model automaton of t_2 is in an execution state". Let A_1 and A_2 respectively the execution states of t_1 and t_2 (actually, the states labelled A of the automaton of figure 4). Then the controller to synthesize must ensure the property

$$Inv(\overline{A_1} \cup \underline{A_2})$$

"Never while" property There again, the property can be straigtforwardly translated in a synthesis objective of invariance state set:

$$Inv(\overline{A_1} \cup \overline{A_2})$$

4.5 Applications

4.5.1 Control automaton for an application

For each application, a control automaton can be constructed. Each declared application has a name, and is launched on the occurence of a signal `req_name`. The automaton of an application named `A` is shown in figure 10. On this figure, the two signals `req_A` and `stop_A` are respectively the requesting signal from the environment to launch the application, and the signal emitted by the application to report its end. It can be launched again at the instant it terminates. This way, the synchronous paradigm is kept: this application can be called in a loop, for example.

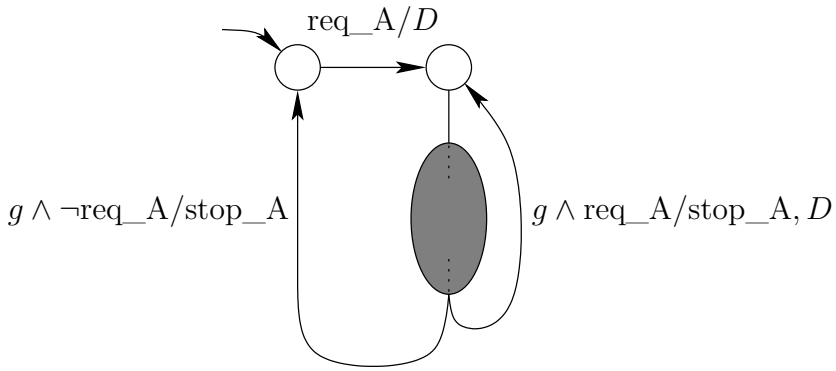


Figure 10: Automaton for a declared application `A`

D and g are respectively a set of requesting signals, and a guard. They are structurally computed from the structure of the body of the application, as well as the core of the automaton, represented in the figure by the grey ellipse. The structural translation uses "proto-automata", an intermediary form of automata, to represent each statement translated, and which will be composed together.

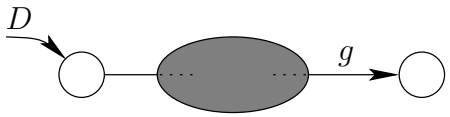


Figure 11: Generic structure of a proto-automaton

A proto-automaton is an automaton as shown in Figure 11, with a labelled initial transition and a "final state" i.e., a sink state, with only one incoming transition, with a guard g and no emission.

- The initial state is the state where the statement *is launched*;
- D is the set of request signals to be emitted at the launch of the statement;
- the final state is where the statement is finished.

In the structural construction, the labelled initial transition, the final state and its incoming transition, will eventually be suppressed in the composition with other proto-automata.

4.5.2 Control automata for statements

Request for a task or application consists in emitting the request, and waiting for the stop, as in Figure 12: the signals "req" and "stop" are respectively the signal requesting the launch of the task (or the application), and the signal reporting its end. The requesting signal is to be emitted immediately, at the first instant of the statement. This statement terminates once the "stop" signal occurs.

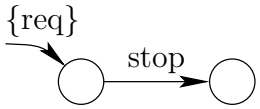
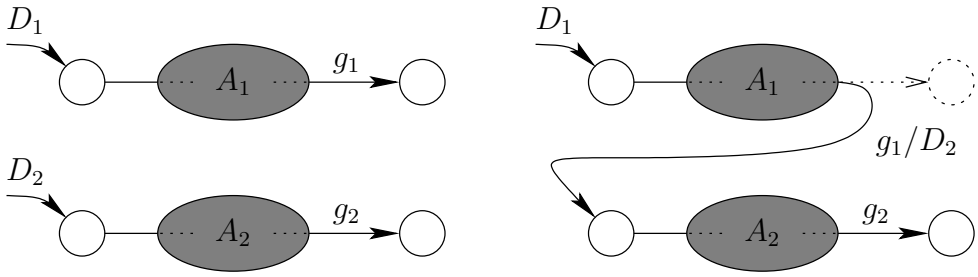


Figure 12: Proto-automaton requesting a task

Sequence of two statements concatenates their proto-automata as in figure 13, representing A_1 ; A_2. The initial state and the initial signals set of the result are those of A_1. When A_1 terminates, requests D_2 for A_2 are emitted, going to the initial state of A_2. The final state is that of A_2. The final state of the A_1 proto-automaton is removed in the structural construction.

Parallel composition The resulting proto-automaton encapsulates the synchronous composition of the composed proto-automata into an initial state. Then, synchronization on termination of all branches causes terminating the parallel construct. Figure 14 gives the result of this contruction.



(a) Proto-automata to be put in sequence

(b) Proto-automaton of the sequence

Figure 13: Sequence of two applications A_1 and A_2

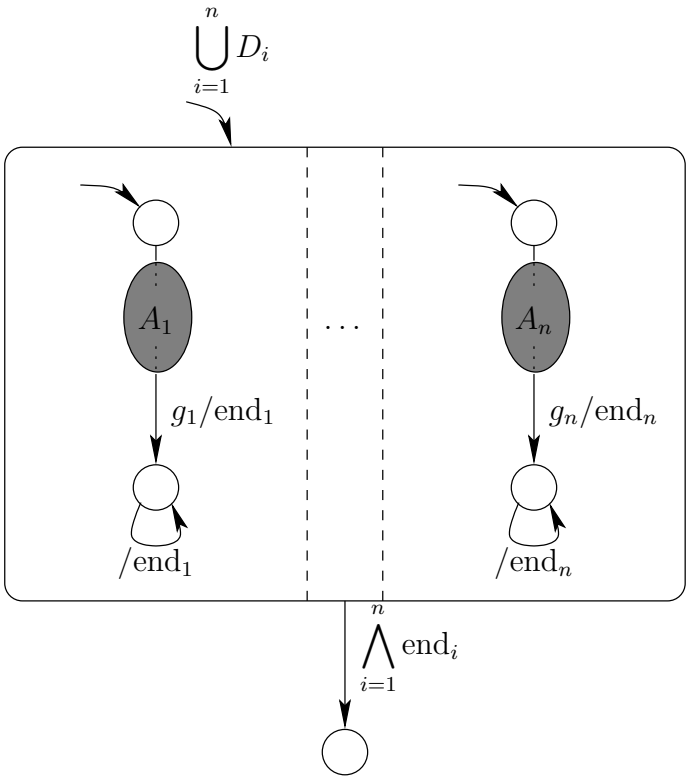
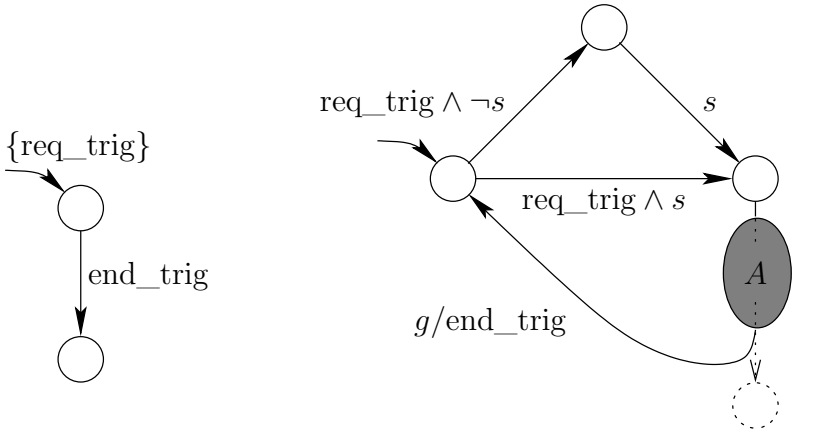


Figure 14: Parallelism of applications A_1 to A_n

Trigger statement. Trigger involves taking into account that the trigger signal can occur at the very instant the statement is launched. Two parallel automata are set up, one for the trigger statement itself (figure 15(a)) and, in parallel, one for the triggered statement (figure 15(b)).

Loop involves the proto-automaton of figure 16. When A terminates, if the signal s isn't present, A is launched again, with emission of signals D.

Alternative Similarly to the trigger, this statement involves two proto-automata: as we have to take into account the signals present at the instant when the application is launched, we have to disjoin the automaton managing the alternative, and the proto-automaton actually representing the application.



(a) Trigger (b) Triggered statement (in parallel)

Figure 15: Triggered statement: A is triggered by s

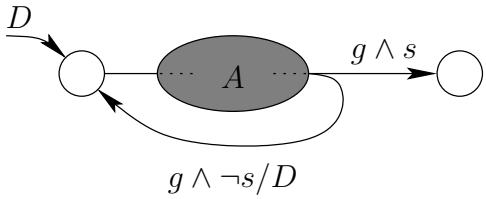


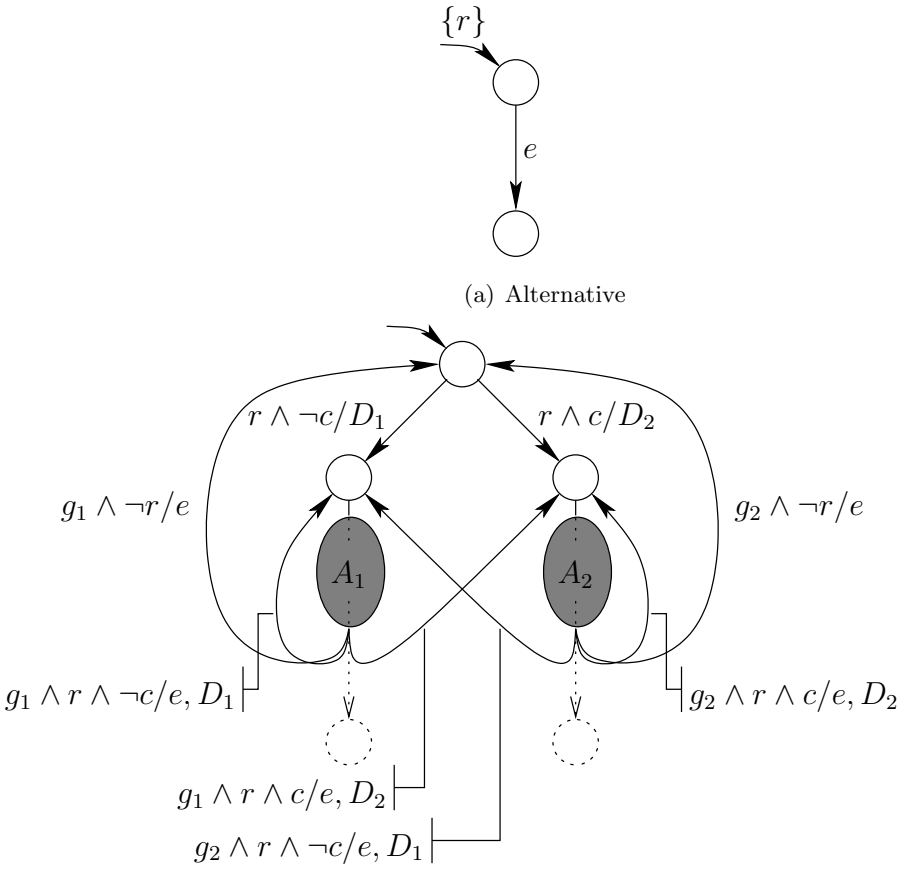
Figure 16: Proto-automaton representing the statement `loop` A `until` s

They represent the statement itself (figure 17(a)), and the alternative between A_1 and A_2 (figure 17(b)), in parallel with the rest of the global application. c is a new controllable signal for the choice of the actually launched statement.

4.6 Global model

For a given NEMO program, a global automaton is built by synchronous composition of all relevant automata, as shown in figure 18. Relevant weight information is associated to states. Also, invariance synthesis objectives are generated, corresponding to the various constraints given by resources and tasks, and observers.

At this level of granularity, abstracting away from the computations in the tasks, the automaton is already quite large. Two perspectives are to be explored: finer grain in modelling the tasks can lead to a finer resolution of the control; better



(a) Alternative

(b) Alternative statements (in parallel)

Figure 17: Alternative between A_1 and A_2

abstractions and compositionality [2] and using coordination code (glue) for some of the properties would alleviate from part of the synthesis cost.

5 Compilation of Nemo: implementation

5.1 Implementation

Nemo is implemented as illustrated in figure 19, which is a concretization of figure 3. The compiler takes a Nemo program, and produces, accordingly to each entity

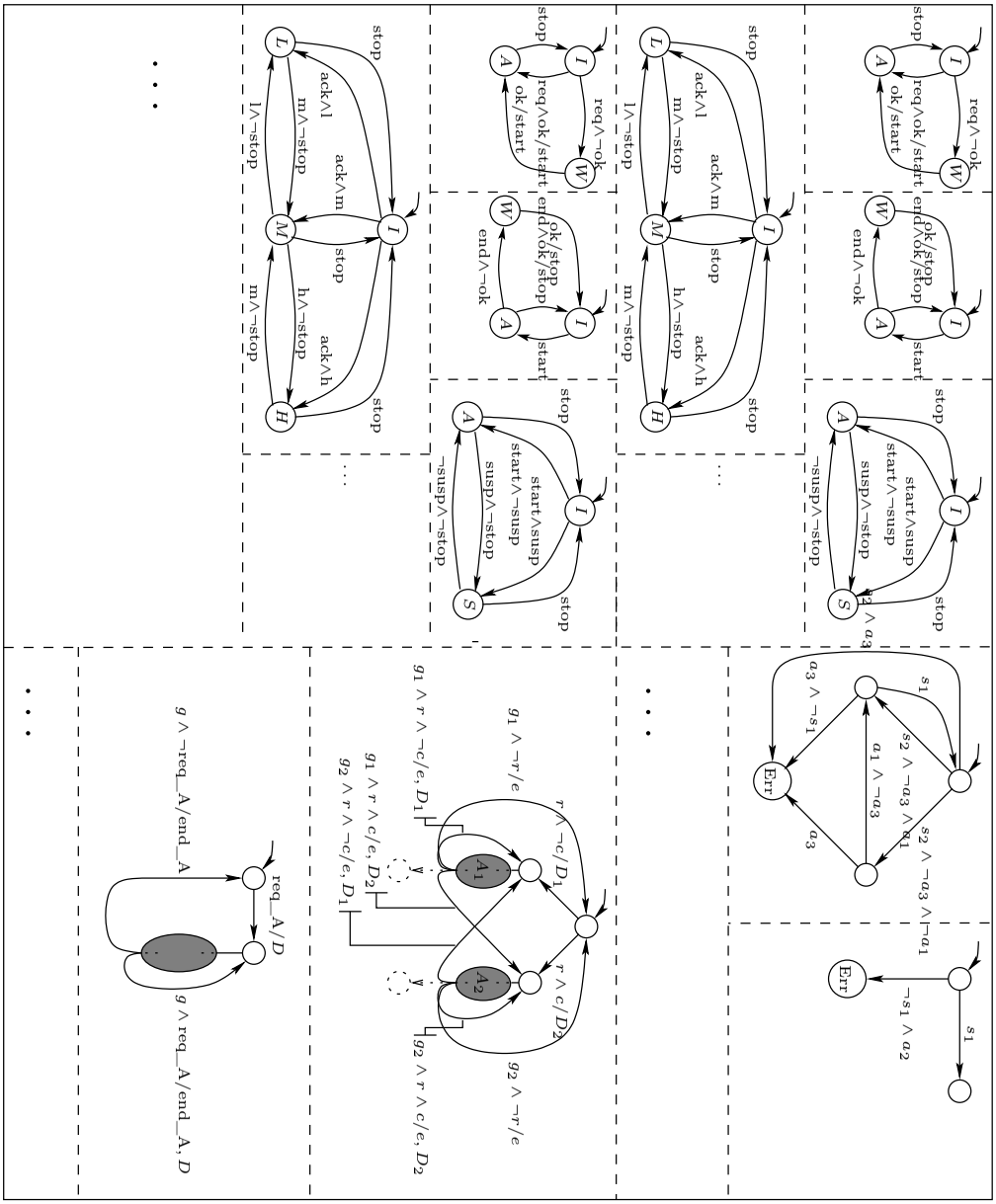


Figure 18: Complete system model

(resource, temporal constraint, task, application), the behavioral parts, in terms of Mode Automata, in its `.targos` syntax, and the more declarative parts, weights and objectives, in terms of the `.z3z` format for the SIGALI tool[1] [19] . The global automaton is compiled using MATOU[2] [17], into a `.z3z` representation, for synthesis purposes, and into the `.ec` format for execution and simulation.

Discrete controller synthesis is performed by SIGALI on the basis of the transition system and the objectives. The resulting controller, available in the `.res` and `.sim` formats, is fed to a resolver, encapsulated into the interactive tool SIGALSIMU [1], wich performs a *co-simulation* of the `.ec` representation with the controller.

[1] `www.irisa.fr/vertecs/Logiciels/sigali.html`
[2] `www-verimag.imag.fr/~synchron`

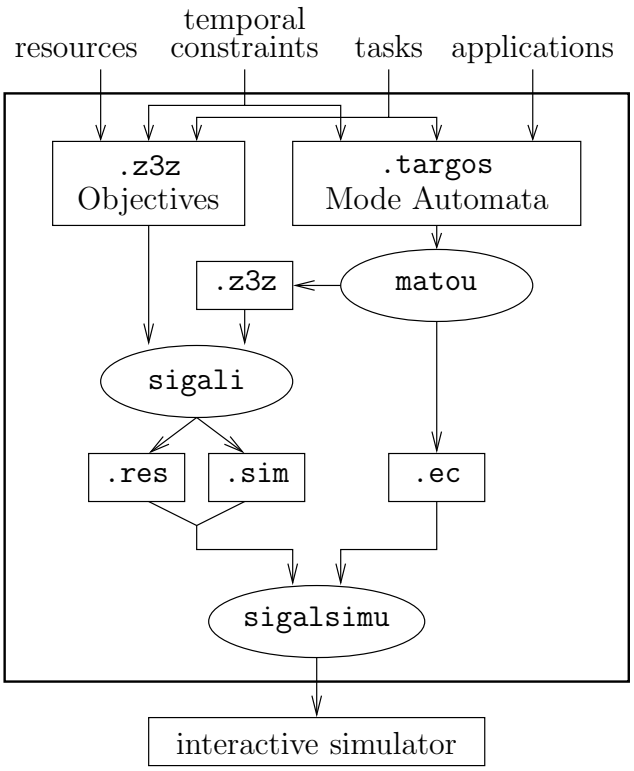


Figure 19: Compilation of NEMO: synchronous tools-based implementation.

5.2 Performances

The significance of our approach strongly depends on the performance of the synthesis tool used. Indeed, while the compilation of the language to automata and synthesis objectives is straigthforward, the actual bottleneck is the discrete controller synthesis, the complexity of which being, just like for model-checking verification, in the worst case polynomial in the size of the state space to handle. The state space of a system produced by the compilation of a NEMO program grows exponentially with the number of tasks and applications, as each of these is modelled by an automaton, and the comprehensive system being the synchronous product of all these automata. It is also to be expected that the performance, in the worst case, will increase dramatically with the size of the model in term of number of tasks and applications. However, we claim that the size of manageable systems is already meaningful, and rising, just like for model-checking verification, especially when compared to what can be achieved brainually.

In order to evaluate the pertinence of the approach, we have measured the time taken by the controller synthesis on models composed of n start-rejectable tasks, for several values of n. The results of this experiment are presented in the following table.

Nb of tasks	1	...	10	...	15	...	20
Synthesis time	0.01s	...	0.34s	...	4.09s	...	4.74s

Nb of tasks	...	23	24	25	26	27	28
Synthesis time	...	4.80s	53min.50s	20.60s	10.79s	9.61s	>24h

Nb of tasks	29	30	31	32	...
Synthesis time	27.88s	24.21s	22.96s	≈19h	...

The actual experimental results presented above show that our approach is relevant for the studied domain, i.e. control systems. The synthesis tool has indeed been able to handle in a few seconds systems composed of more than 30 tasks.

Nevertheless, one can notice several severe losses of performance, e.g. for systems composed of 24, 28 or 32 tasks. Indeed, the computation time of the controller synthesis is difficult to predict, as it rests on manipulation of symbolic equations implemented as BDDs[3]. However, the synthesis time depends on many parameters, several of them being difficult to master, as e.g. the order of the variables. This problem is a recurrent one in the framework of symbolic computation using BDDs, and discussing it further is beyond the scope of this paper; our work can benefit from results of the very active ongoing research in this area.

[3] more precisely, TDDs (Ternary Decision Diagrams) for SIGALI.

Finally, a noteworthy point is that our approach comes as a subsitute to the traditional design/verification/correction one. Thus, even if the discrete controller synthesis operation on some system is not cheap, it is to be reminded that the verification on a similar system would be evenly expensive, as verification and synthesis are based on the same algorithmic basis. The size of the systems possibly managed by the two approach will also be the same. Furthermore, it must be considered that the controller synthesis does provide a solution, and in that sense is to be compared with hours, or days, of brainual design.

6 Typical example

The example proposed below in Figure 20 gathers some of the interesting features of Nemo. The system modelled is a robotic arm aimed at moving some objects from a place to another. The two resources modelled are the actuator (the moving arm), and a CPU. The actuator is obviously an exclusive resource, and we also want its continuous control. The elements of the CPU can be viewed as the percentage of use of it. The system encloses two categories of tasks: `hold_arm` ("default" task holding the arm in its current position), `grab`, `move` and `release` actually manipulate the arm, whereas `check` and `compute_move` are computing tasks. We assume that the objects are brought toward the arm, e.g. by a conveyor belt. Some of these objects are delicate, so at any time, the operator can trigger a checking computation to insure that the system is currently able to handle such objects properly. The event `end_checking` signals that from now, all objects are standard and hence, the check computation won't need to be performed any more.

On this example, the synthesis will compute a controller that will enforce the activation of the `hold_arm` task every time none of the other manipulating tasks is executed.

It will also force the second branch of the alternative of `move_object`, as long as the task `check` can be triggered, because the CPU would not have the capacity to handle the three tasks `compute_move`, `move` and `check` at the same time. This does show the interest of using discrete controler synthesis, as the choice involves a look ahead in the possible paths.

One can also notice that the explicit property "always move between grab and release" won't need any controller synthesis, as it is enforced by the application. In this case, the controller synthesis computation behaves as a verification: if the property is satisfied by the transition system, the controller gives no additional

```
resource actuator_arm:
    exclusive;
    steady control;
end resource;

resource CPU:
    composed of 100 elements;
end resource;

task hold_arm:
    start triggerable,rejectable;
    stop triggerable,rejectable;
    uses actuator_arm, 5 of CPU;
end task;

task grab:
    uses actuator_arm, 20 of CPU;
end task;

task move:
    uses actuator_arm, 20 of CPU;
end task;

task release:
    uses actuator_arm, 20 of CPU;
end task;

task check:
    uses 40 of CPU;
end task;

task compute_move:
    modes
        Precise_move : uses 80 of CPU;
        Rough_move : uses 50 of CPU;
        trans Precise_move <-> Rough_move;
    end modes;
end task;

property
  always move between (grab,release)
end property;

application move_object:
   (grab;(compute_move||move);release)
 | (grab;compute_move;move;release)
end application;

application main:
 loop (move;move_object) until end_app ||
 loop (sig_check triggers check) until end_checking
end application;
```

Figure 20: Example of Nemo program.

constraint. If it hadn't been the case, in another application, the synthesis would have failed, because the tasks are not controllable.

7 Conclusion and prospects

7.1 Results

Results presented are a *domain-specific language*, devoted to multi-task systems, and its *implementation*. Its definition involves a model of multi-task control as transition systems, and the application of *discrete controller synthesis techniques*. The framework is an instance of user-friendly, "hidden" formal method, where the final user need not know about the underlying technicalities.

The approach presented was shown to be well-adapted to the application area considered, i.e. the design of robotic controllers. Indeed, this approach shares many concepts currently manipulated by existing tools of this area, such as ORCCAD where robot controllers are designed by mean of robot-tasks and robot-procedures (sharing the same role as respectively tasks and applications in NEMO). Moreover, the performances of the underlying controller synthesis tool gives good hopes for future scaled applications.

7.2 Prospects

Although the language presented and its implementation are consistent, it is only an outline to suggest what could be an actually useable, maybe more general-purpose language. Therefore, some work still remains.

First short-term prospects concern *usability* of the framework. In the case of absence of solution, the current choice is a short error message pointing out what objective isn't synthesizable. It is worthwhile to think about what kind of diagnosis could be useful to the end users: counter-examples, properties to add or remove in the current model... Also, problems of usability includes *integration* in the aimed application area. Until now, the resulting controller has only a simulable form. A future implementation should be able to connect the resulting controller to a run-time executive, together with computations encapsulated in tasks.

A different and orthogonal concern is the extension of the *multi-tasks system model* used. The reasoning about, e.g., relations between requests and actual beginning of tasks has to be generalized, as its criticalness may depend on the context of the request itself. Model of tasks can for example be extended with notion of successive execution phases, allowing more sophisticated models of tasks to be more easily

described. Given a more specific application area (e.g., fault-tolerant design [8]), model of resources can also be augmented with some ad-hoc primitives in order to allow the built of more elaborated environment models (e.g. where resources can fail or wear off).

Finally, the exclusive use of invariant synthesis objectives may be restrictive, and besides generally leads to a controller still allowing some control (as the controller synthesis computes the *most permissive controller*). In such a controller, choices between eligible values for controllable inputs have to be made at execution time. From this point of view, it could also be interesting to consider other kind of synthesis objectives, qualitative ones such as reachability or attractivity, or quantitative ones such as optimal synthesis on paths. A further study could also be to integrate in the approach some alternatives for the current synthesis tool : solving some constraints with coordination code, or other synthesis techniques such as compositional controller synthesis.

Acknowledgments. We gratefuly acknowledge helpful discussions with and influences by K. Altisen, E. Dumitrescu, G. Gößler, F. Maraninchi, H. Marchand, Y. Rémond.

References

[1] K. Altisen, A. Clodic, F. Maraninchi, and E. Rutten. Using controller synthesis to build property-enforcing layers. In *European Symposium on Programming (ESOP)*, Warsaw (Poland), Apr. 2003. Springer verlag.

[2] K. Altisen, G. Gößler, and J. Sifakis. Scheduler modelling based on the controller synthesis paradigm. *Journal of Real-Time Systems*, 23:55–84, 2002.

[3] A. Benveniste, P. Caspi, S. Edwards, N. Halbwachs, P. L. Guernic, and R. de Simone. The synchronous languages twelve years later. *Proc. of the IEEE, Special issue on embedded systems*, 91(1):64–83, Jan. 2003.

[4] J.-J. Borrelly, E. Coste-Manière, B. Espiau, K. Kapellos, R. Pissard-Gibollet, D. Simon, and N. Turro. The Orccad architecture. *Int. J. of Robotics Research*, 17(4), 1998.

[5] F. Cassez and O. Roux. Compilation of the Electre reactive language into finite transition systems. *Theorical Computer Science*, 146(1-2):109–143, July 1995.

[6] A. Chakrabarti, L. de Alfaro, T. Henzinger, and F. Mang. Synchronous and bidirectional component interfaces. In *CAV 02: Int. Conf. on Computer Aided Verification*, 2002.

[7] P. Darondeau. Verification is autopsy. Personal communication, 29 oct. 2004.

[8] A. Girault and E. Rutten. Discrete controller synthesis for fault-tolerant distributed systems. In *Proc. Ninth Int. Workshop on Formal Methods for Industrial Critical Systems, FMICS 04,* Linz, Austria, 2004.

[9] N. Halbwachs. *Synchronous Programming of Reactive Systems.* Kluwer Academic, 1993.

[10] N. Halbwachs. Synchronous programming of reactive systems, a tutorial and commented bibliography. In *Tenth International Conference on Computer-Aided Verification, CAV'98*, volume 1427 of *LNCS*, Vancouver, Canada, June 1998. Springer Verlag.

[11] N. Halbwachs, F. Lagnier, and P. Raymond. Synchronous observers and the verification of reactive systems. In *Third Int. Conf. on Algebraic Methodology and Software Technology, AMAST'93*, Twente, June 1993.

[12] T. Henzinger, C. Kirsch, and B. Horowitz. Giotto: A time-triggered language for embedded programming. *Proceedings of the IEEE*, 91(1):84–99, January 2003.

[13] L. J. Jagadeesan, C. Puchol, and J. V. Olnhausen. Safety property verification of esterel programs and applications to telecommunications software. In *Computer Aided Verification*, volume LNCS-939, pages 127–140. Springer Verlag, July 1995.

[14] C. Kloukinas, C. Nakhli, and S. Yovine. A methodology and tool support for generating scheduled native code for real-time java applications. In *Third International Conference on Embedded Software (EMSOFT 2003)*, volume LNCS-2855, Philadelphia, Pennsylvania, USA, Oct. 2003. Springer Verlag.

[15] C. Kloukinas and S. Yovine. Synthesis of safe, qos extendible, application specific schedulers for heterogeneous real-time systems. In *15th Euromicro Conference on Real-Time Systems (ECRTS'03)*, Porto, Portugal, 2003.

[16] P. Le Guernic. Compilation involving model-checking and controller synthesis. Personal communication, 1996.

[17] F. Maraninchi and Y. Rémond. Mode-automata: a new domain-specific construct for the development of safe critical systems. *Science of Computer Programming*, (46):219–254, 2003.

[18] F. Maraninchi, Y. Rémond, and E. Rutten. Effective programming language support for discrete-continuous mode-switching control systems. In *Proceedings of the 40th IEEE Conference on Decision and Control, CDC'01,* December 4-7, 2001, Orlando, Florida, pages 3296–3301, 2001.

[19] H. Marchand, P. Bournai, M. Le Borgne, and P. Le Guernic. Synthesis of discrete-event controllers based on the signal environment. *Discrete Event Dynamic System: Theory and Applications*, 10(4), October 2000.

[20] H. Marchand and E. Rutten. Managing multi-mode tasks with time cost and quality levels using optimal discrete control synthesis. In *14th Euromicro Conference on Real-Time Systems (ECRTS'02)*, June 2002.

[21] D. Potop-Butucaru and R. de Simone. Optimizations for faster execution of esterel programs. In *Proceedings of Formal Methods and Models for Codesign, MEMOCODE2003*, June 2003.

[22] P. J. Ramadge and W. M. Wonham. Supervisory control of a class of discrete event processes. *SIAM J. Control Optim.*, 25(1):206–230, 1987.

[23] E. Rutten. *Programmation sûre des systèmes de contrôle/commande : le séquencement de tâches flot de données dans les langages réactifs.* Document d'Habilitation à Diriger des Recherches, IFSIC, Université de Rennes 1, 20 décembre 1999.

[24] E. Rutten and H. Marchand. Automatic generation of safe handlers for multi-task systems. Rapport de Recherche 5345, INRIA, Oct. 2004. www.inria.fr/rrrt/rr-5345.html.

Contents

1 Context and motivation **3**
1.1 Embedded control systems and tasks . . . 3
1.2 Safety-critical systems . . . 3
1.3 Synthesis of task handlers . . . 4
1.4 Our approach . . . 5

2 Analysis of the domain specificities **6**
2.1 Computations, tasks, applications . . . 6
2.2 Resources . . . 7
2.3 The points to be controlled . . . 8
2.3.1 Controlling the termination of a computation . . . 8
2.3.2 Controlling the beginning of a computation . . . 9
2.3.3 Controlling the modes during a computation . . . 9

3 Overview of the language **9**
3.1 Programming multi-tasks systems with Nemo . . . 10
3.2 Resources: implicit properties . . . 11
3.3 Tasks . . . 12
3.3.1 Activity . . . 12
3.3.2 Resources used by a task . . . 13
3.3.3 Modes composing a task . . . 13
3.4 Temporal constraints: explicit properties . . . 14
3.5 Applications . . . 15
3.6 Compiling a Nemo program . . . 17

4 Modelling behaviors and properties **18**
4.1 Preliminary definitions . . . 18
4.1.1 Transition systems . . . 19
4.1.2 Weight functions . . . 19
4.1.3 Discrete controller synthesis . . . 19
4.2 Tasks: behaviours . . . 20
4.2.1 Beginning of the task . . . 20
4.2.2 End of the task . . . 21
4.2.3 Suspensibility of the task . . . 21
4.2.4 Modes . . . 21
4.2.5 Global behavior of the task . . . 23

4.3 Resources: implicit properties and synthesis objectives 23
4.3.1 Notations 23
4.3.2 Synthesis objectives 24
4.4 Temporal constraints: explicit properties 25
4.5 Applications 27
4.5.1 Control automaton for an application 27
4.5.2 Control automata for statements 29
4.6 Global model 31

5 Compilation of Nemo: implementation **32**
5.1 Implementation 32
5.2 Performances 35

6 Typical example **36**

7 Conclusion and prospects **38**
7.1 Results 38
7.2 Prospects 38

List of Figures

1 Control system 6
2 Compilation of Nemo. 10
3 Compilation of Nemo: models and algorithms. 18
4 Models of tasks beginnings 20
5 Models of tasks ends 22
6 Model of the suspension of a task 22
7 Model of three modes of a task 23
8 Complete model of a task 24
9 Observers for the temporal constraints 26
10 Automaton for a declared application `A` 28
11 Generic structure of a proto-automaton 28
12 Proto-automaton requesting a task 29
13 Sequence of two applications A_1 and A_2 29
14 Parallelism of applications A_1 to A_n 30
15 Triggered statement: A is triggered by s 31
16 Proto-automaton representing the statement `loop` A `until` s 31
17 Alternative between A_1 and A_2 32
18 Complete system model 33
19 Compilation of Nemo: synchronous tools-based implementation. . . 34
20 Example of Nemo program. 37

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopˆole de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399